Discrete Mathematics 27 (1979) 297–308

SYNCHRONIZATION AND SIMPLIFICATION

A. de LUCA, D. PERRIN,* A. RESTIVO and S. TERMINI

Laboratorio di Cibernetica del CNR, Arco Felice, Napoli, Italy

Received 23 February 1979

We describe the notions of synchronization and simplification with respect to a given subsemigroup P of a semigroup S in terms of the syntactic semigroup of P. These notions derive from coding theory, which corresponds to the case where P is a free subsemigroup of a free semigroup; we apply the results to give a unified account of several theorems previously published.

0. Introduction

In the theory of codes [5, 11, 14] two concepts are essential: *synchronization* and *simplification*. Suppose we are given an alphabet A; as usual A^+ (resp. A^*) will denote the free semigroup (resp. the free monoid) generated by A. A set X of words over the alphabet A is said to be a *code* if any word over A has at most one decomposition as a product of elements of X; in other terms the set X generates a subsemigroup X^+ of A^+ which is itself free.

A pair (u, v) of elements of X^+ is said to be *synchronizing* if the following condition holds:

$$\forall s, t \in A^*, \quad \{suvt \in X^+ \Rightarrow su, vt \in X^+\}.$$

In other terms a decomposition in words of X of a word w containing the product uv always separates the factors su, vt such that $suvt = w$, whatever be $s, t \in A^*$.

The notion of simplification deals with elements instead of pairs: a word $u \in A^+$ is said to be *simplifying* at right if the following condition holds:

$$\forall x \in X, \qquad \forall t \in A^*, \qquad \{xut \in X^+ \Rightarrow ut \in X^+\}.$$

Thus deciding whether $ut \in X^+$ reduces to deciding whether $xut \in X^+$. The classical problems in coding theory deal with the construction of families of codes satisfying some conditions on synchronization or simplication (cf. [5, 6, 7, 15, 16]).

The aim of this paper is to present a unified treatment of these problems which allow a derivation of previously published results, among which the theorem of Schützenberger [15, 16], answering by the negative a conjecture of Gilbert and

* Laboratoire Informatique Theorique et Programmation, LA 248, Université de Rouen, France.

Moore [5], and asserting that for a finite code which is maximal (as a code), either all words are simplifying, or there exist arbitrarily long ones which are not.

We have tried everywhere possible to weaken the hypotheses and to formulate the results in the broader possible framework. Such a presentation is useful for our purpose since it treats at the same time the situation in the free semigroup and the corresponding one in the syntactic semigroup.

In a first paragraph, we recall some results and definitions needed below. For semigroups, we use the notation of [2] and for automata theory that of [4].

In Section 2, we give the syntactic characterization of synchronizing pairs; this allows, in particular, an algorithm to find such pairs. Turning in Section 3 to the case of a free semigroup, we give a characterization of subsemigroups with bounded synchronization delay which yields a proof of a result from [12].

We give in Section 4 the definition of simplifying elements and their syntactic characterization. This is applied in Section 5 to give a simplified presentation of Schützenberger's theorem on deciphering delay for maximal codes.

1. Preliminaries

Given a subset P of a semigroup S, the *syntactic congruence* of P is the maximal congruence of S such that P is a union of congruence classes. It is well known (cf. [2]) that this congruence is defined as follows:

$$s \equiv t \bmod P \quad \Leftrightarrow \quad \{\forall u, v \in S^1, \qquad usv \in P \quad \Leftrightarrow \quad utv \in P\},$$

where S^1 is obtained by adding an eventual neutral element to S. The quotient of S by this congruence is the *syntactic semigroup* of P, denoted as $S(P)$ and the canonical morphism

$$\eta : S \to S(P)$$

is the *syntactic morphism*. We shall denote by ϕ^1 the morphism of monoids from S^1 onto $S^1(P)$.

A subset P of S is said to be *disjunctive* if its syntactic congruence reduces to the identity. If follows that the homomorphic image of an arbitrary subset P of S in its syntactic semigroup $S(P)$ is a disjunctive subset of $S(P)$.

A subset P of S is said to be *dense* if it intersects all the two-sided ideals of S.

If P is not dense, then $S(P)$ has a zero which is the image of the maximal ideal of S having an empty intersection with P.

Proposition 1.1. *Let S be a semigroup admitting a nondense disjunctive subsemigroup P. Then, if there exists a 0-minimal ideal of S, it is unique.*

Proof. First P meets every 0-minimal ideal J in S, since, otherwise, $J = 0$; further, for any pair J, K of 0-minimal ideals, let $p \in J \cap P$, $q \in K \cap P$. Then the product pq is not zero since it belongs to P, whence $pq \in J \cap K$ and $J = K$. □

A subset P of S is called *recognizable* if $S(P)$ is finite. It is well known that, in particular, a finitely generated subsemigroup of a free semigroup is recognizable [4]. We deduce from the above statements that, for a recognizable subsemigroup P of S, either P is dense and $S(P)$ admits a minimal ideal that meets $P\phi$, either P is nondense and $S(P)$ admits a unique 0-minimal ideal.

We shall make here the convention that we only consider *nondense* subsemigroups P (except where explicitly stated); this is not a restriction of generality since one may always add a zero to the semigroup S.

In the case of a disjunctive subsemigroup P of S, the condition that P is nondense implies that S has a 0.

Let P and Q be subsets of S. We use the notations $P^{-1}Q$ and QP^{-1} to denote the sets

$$P^{-1}Q = \{s \in S \mid Ps \cap Q \neq \emptyset\} \quad \text{and} \quad QP^{-1} = \{s \in S \mid sP \cap Q \neq \emptyset\}.$$

A subsemigroup P of S is called *free in* S (*liberable* in french) if and only if $P^{-1}P \cap PP^{-1} \subset P$. If S is the free semigroup generated by a set A, a classical result of Schützenberger [14] shows that a subsemigroup P of A^+ is free if and only if P is free in A^+.

We now state and prove a series of more or less classical lemmas to be used in the sequel. The first one deals with the computations in the 0-minimal ideal;

Lemma 1.2. *Let P be a disjunctive subsemigroup of a finite semigroup S and $J' \subset J$ be the union of 0-minimal right ideals intersecting P. Then $P^{-1}P \cap J' \subset P$.*

Proof. Let $s \in P^{-1}P \cap J'$; this implies by definition the existence of $p \in P$, $q \in P \cap J$, $t \in S$ such that: $ps \in P$ and $s = qt$.

Now qpq is in P and in the $\mathcal{H}$-class of q; we may find an element r in P such that: $q = rqpq$; one then has:

$$s = qt = rqpqt = rqps.$$

But, since $r, q, ps \in P$, this implies $s \in P$, as asserted. □

The second result deals with the case where P is a subsemigroup of the free semigroup A^+ over the set A. It holds back to Schützenberger (cf. [18]).

Lemma 1.3. *If $P \subset A^+$ is finitely generated, then $P\phi$ meets every regular $\mathcal{D}$-class in $S(P) \setminus 0$.*

Proof. Let e be an idempotent in $S(P)$ *and* $w \in e\phi^{-1}$. If $e \neq 0$, there exist $u, v \in A^*$ such that $uwv \in P$ and thus:

$$\forall k \geq 1, \qquad uw^k v \in P.$$

Now let l be the maximal length of the words of a finite set X of generators of P; we may suppose that $|w| > l$. This implies that, in the factorization of $uw^k v$ in a product of elements of X, each factor w contains an occurrence of this factorization:

$$uw_{i_1}, \qquad w_{j_1}w_{i_2}, \ldots, w_{j_{k-1}}w_{i_k}, \qquad w_{j_k}v \in P,$$

with

$$w_{i_n}w_{j_n} = w, \quad \text{for} \quad 1 \leqslant n \leqslant k.$$

If we further choose $k > |w|$, there exist distinct integers n,m, $1 \leqslant n$, $m \leqslant k$, such that

$$w_{j_n} = w_{j_m}.$$

We thus obtain a factorization $w = w'w''$ (with $w' = w_{i_n} = w_{i_m}$) such that

$$uw^p w', \qquad (w''w')^q, \qquad w''w^r v \in P$$

with $p+q+r = k-1$. Now either $q = 1$ and $w''w' \in P$; either $q \geqslant 2$ and

$$(w''w')^2\phi = w''\phi e w'\phi = w''\phi e^{q-1}w'\phi = (w''w')^q\phi \in P\phi.$$

In both cases $f = (w''w')^2\phi$ is in $P\phi$ and idempotent; moreover

$$f \mathscr{L} w'\phi \mathscr{R} e$$

so that e and f lie in the same $\mathscr{D}$-class. □

We shall also need the following elementary fact whose proof is left to the reader (cf. [4, p. 81]).

Lemma 1.4. *If all the idempotents of a semigroup S are contained in a two-sided ideal I of S, then $S^k \subset I$, where*

$$k = \text{Card}\,(S \setminus J) + 1.$$

2. Synchronization

Let P be a disjunctive subsemigroup of a finite semigroup S and consider the intersection of P with the 0-minimal ideal J of S; we have already seen that it is not empty, and it must also contain an idempotent since it is a subsemigroup. Therefore P meets a maximal subgroup G of J and $H = G \cap P$ is a subgroup of G.

Proposition 2.1. *Any normal subgroup of G contained in H is trivial.*

Proof. Let N be a normal subgroup of G contained in H and thus in P. Denote by e the idempotent of G and by n an arbitrary element of N. We show that: $n \equiv e \bmod P$; which implies $n = e$ since P is disjunctive. Suppose that, for $u, v \in S^1$, one has $unv \in P$ and set:

$$u' = eue, \qquad v' = eve.$$

One then has: $u'nv = e(uenv) = e(unv) \in P$, and a symmetrical argument shows that $unv' \in P$; therefore both u' and v' are nonzero and thus in G. Using now the fact that N is normal in G, we get for some $m_1, m_2 \in N$:

$$u'nv = m_1 u'v \in P, \qquad unv' = uv'm_2 \in P.$$

Thus: $u'v = m_1^{-1}u'nv \in P$ and $uv' = unv'm_2^{-1} \in P$, whence $euev$ and $ueve$ belong to P; this implies $uev \in P$ by Lemma 1.2. Conversely, if $uev \in P$, then one just has to reverse the implications to get $unv \in P$, concluding the proof. □

Proposition 2.1 shows that the representation of G over the (right) cosets of H is faithful. The different representations obtained by choosing different maximal subgroups G in J are well known to be equivalent. The degree of this representation, which is the index of H in G is by definition, the degree of synchronization or *degree* of P. For the general case where $S \neq S(P)$, the degree of P will be that of its image in $S(P)$.

A subsemigroup P of degree 1 is called *synchronizing*. As a corollary of Proposition 2.1, it follows that P is synchronizing if and only if the structure group of J is trivial.

Following Schützenberger [16], we define a *constant* in a semigroup S with respect to a subset P of S as an element $c \in S$ such that

$$ucv,\ wcx \in P \ \Rightarrow \ ucx \in P$$

for any (u, v, w, x) in S^1. We then have

Proposition 2.2. *For a disjunctive subsemigroup P of a finite semigroup S the following conditions are equivalent.*

(1) *P is synchronizing.*
(2) *S admits nonzero constants with respect to P.*
(3) *The structure group of J is trivial.*

In this case, the constants are precisely the elements of J.

Proof. We have already seen that (1) and (3) are equivalent. Further if P is synchronizing, let c be an element of J and suppose that ucv, wcx, with

$u, v, w, x \in S^1$ are in P. Then, since the structure group of J is trivial $ucx = (ucv)(wcx)$ is in P and c is a constant. Reciprocally, if $c \neq 0$ is a constant, then for any u, s, v in S^1, one has

$$ucscv \in P \quad \Rightarrow \quad ucv \in P$$

and, conversely if $ucv \in P$ and $csc \neq 0$ one has $ucscv \in P$ since there exists at least $w, x \in S^1$ such that $wcscx \in P$ and this implies $ucscx \in P$ and then since c is a constant $ucscv \in P$. Finally, for any s in S^1, being P disjunctive csc is either equal to c or to zero; since $c \neq 0$ one derives that c belongs to the 0-minimal ideal of S, and this ideal has a trivial structure group since cSc is equal to the union of zero and the $\mathcal{H}$-class of c; whence P is synchronizing and the proof is concluded. □

The definition of constants is closely related to that of *synchronizing pairs*; a pair (f, g) of elements of a subsemigroup P is said to be synchronizing if the following implication holds for any u, v in S^1:

$$ufgv \in P \quad \Rightarrow \quad uf, gv \in P.$$

Thus, if (f, g) is a synchronizing pair, the product fg is a constant and, conversely, if f and g are constants and in P, the pair (f, g) is synchronizing.

3. Delay of synchronization

The delay of synchronization of a subsemigroup P in A^+ is the least integer n (finite or not) such that any pair in $P^n \times P^n$ is synchronizing.

We assume now P to be recognizable and we investigate for the consequences on the syntactic semigroup $S = S(P)$ of a finite synchronization delay.

Proposition 3.1. *A sufficient condition for P to have finite synchronization delay is that, for any idempotent e in S, one has*

$$eSe = \{e, 0\}.$$

This condition is also necessary if P is finitely generated.

Proof. Let $n = \mathrm{Card}(S \setminus J) + 1$; then any element f in $A^n A^*$ has its image in J by Lemma 1.4, since the condition $eSe = \{e, 0\}$ for all idempotents is equivalent to the fact that all the idempotents of S are in J and that the structure group of J is trivial. From Proposition 2.2 we deduce that all the elements of $A^n A^*$ are constants, achieving the proof of the sufficiency.

Now if P is finitely generated and has finite synchronization delay let e be an idempotent in $S \setminus 0$; then by Lemma 1.3 there exists an idempotent $f \in P\phi$ in the $\mathcal{D}$-class of e; since f is a constant one has $f \in J$ and then $e \in J$. As the structure group of J is trivial it follows $eSe = \{e, 0\}$. □

The condition of Proposition 3.1 is not necessary in general, as shown by the example of the subsemigroup generated by the set:

$$X = (a^2)^* b.$$

The subsemigroup P has a delay of synchronization equal to 1 since b is a constant. However $a^2\phi$ is an idempotent lying outside of J.

We deduce from Proposition 3.1 the following result, due to Restivo [12].

Corollary 3.2. *Let P be a finitely generated subsemigroup of A^+. Then P has a finite synchronization delay iff there exist four finite subsets F, U, V, W of A^+ such that*

$$P = F + (UA^* \cap A^*V) \setminus A^*WA^*$$

Proof. If P is given as above and l is the maximum of the lengths among the words of F, U, V, W, then any $c \in P^{l+1}$ is a constant since

$$ucv, wct \in P \quad \Rightarrow \quad uc \in UA^*, \qquad ct \in A^*V, \qquad uct \notin A^*WA^*,$$

and thus one has $uct \in P$ showing that c is a constant with respect to P. Conversely, if P is finitely generated and has finite synchronization delay l let J be the 0-minimal ideal of $S = S(P)$. Let F be the complement in P of the set $R = (P\phi \cap J)\phi^{-1}$, so that

$$P = F + R.$$

Now any word $f \in P^{2l}$ belongs to the second term in the sum since it is a constant. Thus F is finite being P finitely generated. We now define

$$T = 0\phi^{-1}, \qquad U = R \setminus RA^+, \qquad V = R \setminus A^+R,$$
$$W = T \setminus (A^*TA^+ \cup A^+TA^*).$$

So that W is the basis of the two-sided ideal T and U (resp. V) is the basis of the right (resp. left) ideal generated by R. Then

$$R = (UA^* \cap A^*V) \setminus A^*WA^*.$$

In fact, R is obviously contained in the right hand side of this equality. And, conversely, for any u, v in R, one has

$$uA^* \cap A^*v \subset R \cup T$$

since the structure group of J is trivial.

It remains to show that U, V, W are finite. Let $k = \text{Card}\,(S \setminus J) + 1$ and t be the maximal length of the words of X (the unique minimal set of generators of P). Let us show that the length of the elements of U is bounded by $k + t$. In fact, if $u \in U$

and $|u| \geq k + t$ we may write $u = xy$ with $x \in P$, $y \in X$ and $|x| \geq k$. Then $x\phi$ belongs to J by Lemma 1.4 and this contradicts the definition of U. The set U is therefore finite, and so is V, symmetrically.

Now if $w \in W$ and $|w| \geq k + 2$, let us write $w = aw'b$ with $a, b \in A$. Since $|w'| \geq k$, the image $w'\phi$ is in J; but if $w'\phi = 0$, $w \in ATA$, a contradiction; in the same way, one has $aw'\phi, w'b\phi \neq 0$. Now this implies that $aw'\phi$ (resp. $w'b\phi$) generates the same left (resp. right) ideal as $w'\phi$ and we can find u, v in A^+ such that

$$uaw'\phi = w'\phi, \qquad w'bv\phi = w'\phi.$$

Then,

$$uwv\phi = uaw'bv\phi = w'bv\phi = w'\phi = 0$$

in contradiction with the hypothesis. Thus W is also finite and the proof is complete. □

4. Deciphering delay

Let P be a subsemigroup of S; we say that an element s of S is (right)-*simplifying* if

$$\forall p \in P, \qquad \forall t \in S^1, \quad \{pst \in P \quad \Rightarrow \quad st \in P\}.$$

For instance, if P is left unitary (that is to say $P^{-1}P \subset P$), then any element of S is simplifying and viceversa. In the general case the set U of simplifying elements is a right ideal and one has

Proposition 4.1. *Let P be a disjunctive subsemigroup of a finite semigroup S. Then any element generating a 0-minimal right ideal intersecting P is simplifying.*

Proof. This is just another way of stating Lemma 1.2. □

Now the *deciphering delay* of P is the least integer d (finite or not) such that any element in P^d is simplifying. A delay of deciphering equal to zero will mean that P is left unitary.

Turning to the case where $S = A^+$, the free semigroup over A, one realizes that the deciphering delay of P gives the minimal number of generators of P that one has to wait in a left-right reading of a word in order to be able to reduce the problem of $u \in P$ to that of $pu \in P$ knowing that $p \in P$.

The deciphering delay is always less than or equal to the delay of synchronization. In fact, if n is the delay of synchronization of P and

$$p \in P, \qquad q \in P^n, \qquad pqt \in P,$$

then $p^n qt \in P$, so that $qt \in P$ and q is simplifying.

Now let us define a *strongly right-completable* element as an $s \in S$ such that for any $t \in S^1$, either st is such that

$$PstS^1 \cap P = \emptyset$$

or it is right-completable, i.e.

$$stS^1 \cap P \neq \emptyset.$$

Denote by V the right ideal of all strongly right completable elements of S.

Proposition 4.2. *Let P be a subsemigroup of S. One has the inclusion $U \subset V$. Moreover if P is a disjunctive subsemigroup of a finite semigroup S, free in S, then $V \subset U$.*

Proof. Let $u \in U$ and $t \in S^1$. Then either $Put\ S^1 \cap P = \emptyset$ or, alternatively, there exist $p \in P$ and $t' \in S^1$ such that $putt' \in P$. Since u is simplifying it follows that $utt' \in P$. Thus $u \in V$.

Let now P be a disjunctive subsemigroup of a finite semigroup S free in S (i.e. $P^{-1}P \cap PP^{-1} \subset P$) and denote by J the 0-minimal ideal of S. Let $v \in V$. If $PvS^1 \cap P = \emptyset$, then $v \in U$. Otherwise let $p \in P$, $t \in S^1$ be such that $pvt \in P$. Choosing $x \in P \cap J$, the right-ideal generated by vtx is 0-minimal and it intersects P since $v \in V$; thus we may find u in this ideal such that $vtxu \in P$. But, by Lemma 1.2, one has $u \in P$ since $u \in J'$ and $pvtx$, $pvtxu \in P$. As pvt, $vtxu \in P$ and since P is free in S it follows that $vt \in P$ which shows that $v \in U$. □

Proposition 4.3. *Let P be a recognizable subsemigroup of A^+. If U is finitely generated then P has a bounded deciphering delay. If P is a dense finitely generated subsemigroup of A^+ having a bounded deciphering delay then U is finitely generated.*

Proof. First, if U is finitely generated, let d be the maximum length of the elements of the base B of U; if $p \in P^d$, then p is in U: for, if $q \in P$ is such that its syntactical image $q\phi$ generates a 0-minimal right ideal, then so does $pq\phi$, so that pq is simplifying by Proposition 4.1 and it is also strongly right completable from Proposition 4.2; now as $pq = bc$, with $b \in B$, $c \in A^*$, it follows from $|p| \geq d \geq |b|$ that p belongs to U as asserted. Whence the delay of P is at most d. This concludes the proof of the first part of the proposition.

We suppose now that P is a dense, finitely generated subsemigroup of A^+ having a bounded deciphering delay d. Let u be an element of U whose length exceeds dk: $|u| \geq dk$, where k is the maximal length of the words of the minimal generating set X of P. Since P is dense one easily derives that $PuA^* \cap P \neq \emptyset$ so that u is right completable in P. Thus u can be written as

$$u = x_1 x_2 \cdots x_d w$$

with $w \in A^*$ and $x_i \in X$, $1 \leq i \leq d$. But $x_1 x_2 \cdots x_d$ is, by definition of d, simplifying; hence the right ideal U is generated by words of length at most dk. □

5. Maximal codes

We now turn to the case where the semigroup P is *dense* in S, that is to say that it meets any ideal of S.

We shall also deal with a *free* subsemigroup P of the free semigroup A^+; its minimum generating set X is called a *code* and it is well-known that, provided X is nondense, $P = X^+$ is dense iff X is maximal as a code (on these problems see [4]).

We give here, using the previous notations, a proof of the following result which is essentially the same as that of [15, 16].

Theorem 5.1. (Schützenberger). *Let X be a finite maximal code; then the deciphering delay of X^+ is either 0 or infinite.*

Proof. Let S be the syntactic semigroup of $P = X^+$ and J be its minimal ideal. Choose a word $x \in P$ such that $x\phi \in J$ and denote by F the set of words $f \in A^*$ such that $xf \in P$ and by H the set $F \setminus FP$. H is a finite set since it is formed by the right factors of the words of the set X.

Let now U be the set of the simplifying elements of A^+ and B its base as a left ideal.

Since P is free dense and finitely generated it follows from Proposition 4.2 that $U = V$ and from Proposition 4.3 that P has a bounded deciphering delay if and only if B is finite. Let us now prove the following lemma (cf. [15, p. 221]).

Lemma 5.2. *For any word $s \in A^+$, there exists at least one pair $(h, b) \in H \times B$ such that s is a left factor of a word in hbA^* and at most one such that hb is a left factor of s.*

Proof. For any $s \in A^+$, the word xs is right-completable so that

$$xsv \in X^+$$

for a $v \in A^+$. Hence we may write $sv = hv'$ with $v' \in X^*$ and since P is free $h \in H$; and as $v'x$ is in U, the word svx has at least one left factor in HB.

Now if $hbf = h'b'f'$, with $h, h' \in H$, $b, b' \in B$ and $f, f' \in A^*$, let $v \in A^+$ be such that $bfv \in X^+$; one then has

$$(xh)(bfv) = (xh')(b'f'v)$$

with each word between parenthesis belonging to X^+ since b' is simplifying. As X^+ is free this implies $h \in h'X^*$ and finally $h = h'$. □

Now let π be the natural morphism of A^* into the ring R of polynomials in commuting variables $a \in A$, coefficients in Z, taken modulo the polynomial $\sum_{a \in A} a - 1$. It is well known that the conclusions of Lemma 5.2 imply $\pi(HB) = 1$ together with $\pi(HB) = \pi(H)\pi(B)$; but as H and B are finite, the equality

$$\pi(H)\pi(B) = 1$$

implies $\pi(H) = \pi(B) = 1$. Now $\pi(B) = 1$ implies that any word in A^+ is a left factor of some word in $BA^* = U$; this means that any word in A^+ is right completable and this leads to $U = A^+$. Finally any word is simplifying and X^+ has deciphering delay zero, as asserted. □

As it is well known [4] the basis X of a left unitary subsemigroup of A^+ is a *prefix* code. Symmetrically X is said to be *suffix* if X^+ is right unitary (i.e. $PP^{-1} \subset P$) and *biprefix* if X^+ is right and left unitary.

The following corollary is proved in [9] under stronger hypotheses; the only if part holds back to Schützenberger (cf. [9]).

Corollary 5.4. *Let X be a finite maximal code. It is biprefix iff the syntactic semigroup S of X^+ has no idempotent outside its minimal ideal.*

Proof. First, if X is biprefix, let e be an idempotent in S and let $s \in e\phi^{-1}$ be chosen longer than any word of X. Denote as I (resp. F) the set of left (resp. right) factors of s which are right (resp. left) factors of some element of X; more precisely

$$I = \{i \in A^* \mid s \in iA^*;\ A^+ i \cap X \neq \emptyset\}.$$

Now, for a given word $w \in A^+$, we define a mapping from I to F as follows: to any $i \in I$, there corresponds a unique $f \in F$ such that

$$sws = ixf, \qquad x \in X^*,$$

and conversely any such f defines a unique i satisfying this property. Moreover, for each $f \in F$, there exists a unique $i \in I$ such that $fi \in X$; these two facts imply the existence of an integer n such that, for each $i \in I$, one has

$$(sws)^n = iyf, \qquad y \in X^*, \qquad fi \in X,$$

But this just means that $(sws)^n \equiv s$ and proves the only if part.

Reciprocally if all the idempotents of S belong to J then by making use of Lemma 1.4 and of the fact that $U = V$ one can easily derive that U is finitely generated. This implies, from Proposition 4.3, that X has a finite deciphering delay and thus delay zero by Theorem 5.1. Symmetrically by using a similar argument from right to left one derives that X has to be suffix and this concludes the proof. □

References

[1] J.M. Boë, Representations des monoïdes; applications à la theorie des codes, Thèse de 3 Cycle, Montpellier (1976).
[2] A.H. Clifford and G.B. Preston, The Algebraic Theory of Semigroups, Amer. Math. Soc. Vol. 1 (1961), Vol. 2 (1967).
[3] A. De Luca, On some properties of the syntactic semigroup of very pure subsemigroups, R.A.I.R.O., I.T. (1979), in press.
[4] S. Eilenberg, Automata, Languages and Machines, Vol. A (1974), Vol. B (1976) (Academic Press New York).
[5] E.N. Gilbert and E.F. Moore, Variable length binary encodings, Bell Syst. Techn. J. 38 (1959) 933–967.
[6] S.W. Golomb, and B. Gordon, Codes with bounded synchronization delay, Information and Control 8 (1965) 355–372.
[7] L.J. Guibas, and A.M. Odlyzko, Maximal prefix synchronized codes, to appear in SIAM J. on Appl. Math. (1978).
[8] R. McNaughton, and S. Papert, Counter Free Automata (MIT Press, New York, 1971).
[9] D. Perrin, Codes biprefixes et groupes de permutations, These de doctorat d'etat, Université de Paris VII (1975).
[10] D. Perrin, Codes asynchrones, Bull. Soc. Math. de France, 105 (1977) 385–404.
[11] J.F. Perrot, La theorie des codes à longueur variable, in: Lecture Notes in Computer Science 48 (Springer Verlag Berlin, 1977) 27–44.
[12] A. Restivo, On a question of McNaughton and Papert, Information and Control 25 (1974) 93–101.
[13] J. Sakarovitch, Monoïdes syntactique et langages algebriques, Thése 3 Cycle, Université Paris VII (1976).
[14] M.P. Schützenberger, On an application of semigroup methods to some problems in coding, IRE Trans. Information Theory I.T. 2, (1956) 47–60.
[15] M.P. Schützenberger, Sur certains sous-monoïdes libres, Bull. Soc. Math. de France 93 (1965) 209–223.
[16] M.P. Schützenberger, On a question concerning certain free submonoids, J. Combinatorial Theory 1 (1966) 437–442.
[17] M.P. Schützenberger, Sur certaines operations de fermeture dans les langages rationnels, Symposia Mathematica XV (1975) 245–253.
[18] M.P. Schützenberger, A property of finitely generated submonoids of free monoids, in: G. Pollak, ed., Proc. Colloq. on Algebraic Theory of Semigroups, 1976. Szeged (Hungary). Colloquia Mathematica Societatis János Bolyai (North Holland, Amsterdam).